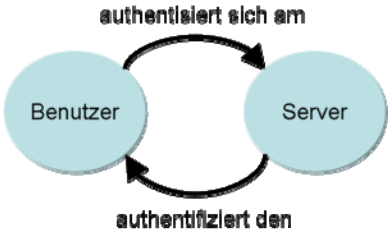
Hinweise zum Verfahrensverzeichnis paedML Teil 2

10. technische und organisatorische Maßnahme nach § 9 LDSG

Merkmal	**Beschreibung**
1.Zutrittskontrolle: → Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren	1) Wie werden die Gebäude/ Räume (Serverraum, Verteilerraum) abgesichert? Hinweis: Der Serverraum (im Gebäude ….) sowie der Verteilerraum (im Gebäude ….) sind jeweils durch ein separates Schloss gesichert. Beide Räume sind immer abgeschlossen.
Hinweis: physischer Zugang zu den Räumen	2) Wer hat wann wohin Zutritt zu diesen Räumen? Hinweis: Zutritt zum Serverraum bzw. Verteilerraum hat nur die von der Schulleitung benannte Lehrkraft sowie der Hausmeister und Mitarbeiter des Schulträgers. Der Zutritt ist zeitlich nicht beschränkt. Der Zutritt ist werktags nur von 7.00 bis 18 Uhr möglich. → http://lehrerfortbildung-bw.de/sueb/recht/ds_neu/vwpd/
	3) Wird die Zutrittskontrolle durch weitere organisatorische/technische Maßnahmen unterstützt? - Beschreibung des Schlüsselmanagements (Reinigungsdienst / Mitarbeiter / Ferien) Hinweis: Die Schlüssel werden über das Sekretaritat verwaltet. Die Schlüsselinhaber werden namentlich in einer Liste geführt. - Serverraum im EG (Fensterabsicherung / Klimaanlage) Hinweis: Da sich der Server im EG befindet wurde im Raum ein Klimaanlage angebracht. Das Fenster ist immer verschlossen und wurde mit einem Außengitter abgesichert.
2. Datenträgerkontrolle → zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können	1) Welche Datenträger sind erforderlich? Hinweis: Festplatten für den Server; USB-Festplatten für die wöchentliche Sicherung; NAS-Geräte um große Dateien auslagern zu können.
Hinweis: physischer Zugriff auf die Datenträger des Servers bzw. der Datensicherung	2) Wie wird die Nutzung von Datenträgern (z.B. USB-Stick) technisch beschränkt? Hinweis: Die Nutung von Datenträgern ist technisch nicht beschränkt damit die Schüler und Lehrer mit Hilfe persönlicher USB-Sticks Ihre Sicherung mit nach Hause nehmen können.
	3) Wer ist für die Datenträger verantwortlich? Hinweis: Für die Datenträgerverwaltung (Serverfestplatten, USB-Sicherungsplatten) ist die von der Schulleitung benannte Lehrkraft (Netzwerkberater / Standortbetreuer) verantwortlich.
	4) Wo werden die Datenträger aufbewahrt? Hinweis: Server-Bereich: Die Datenträger mit personenbezogenen Daten inkl. der Festplatten mit der Datensicherung befinden sich ausschließlich im Serverraum / in einem separaten Brandabschnitt (Safe der Schulleitung) der entsprechend gesichert ist (siehe Anlage).

Merkmal	Beschreibung
	5) Welche Datenträger werden verschlüsselt (Verschlüsselungstiefe)? Hinweis: Die Serversicherung liegt aufgrund des Imageverfahrenes in komprimierter Form vor. Die Sicherung der Home- / Tauschverzeichnissen erfolgt unverschlüsselt.
	6) Wie wird mit Datenträgern verfahren, die entsorgt werden müssen? Hinweis: Mehrmaliges Formatieren mit US Government Methode (4 x mit verschiedenen Bitmustern beschrieben) http://www.br-online.de/ratgeber/festplatte-loeschen-sicherheit-ID1279193979496.xml http://eraser.heidi.ie/index.php http://www.dban.org
3.Speicherkontrolle → die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern Hinweis: paedML Benutzerdatenbank sowie Daten und Dateien auf dem Server bzw. auf externen Speichersystemen (SAN) Begriffe[1] Identifizierung: Vorgang, der zum eindeutigen Erkennen einer Person Authentifizierung  Die eine Authentifizierung abschließende Bestätigung wird auch als Autorisierung bezeichnet.	1) Welches Verfahren zur Identifizierung und Authentifizierung wird verwendet? → siehe Anlage LMZ paedML Hinweis: Sie erfolgt über eine individuelle Benutzerkennung mit persönlichem Passwort
	2) Werden zugangsgeschützte Zugriffe protokolliert? In welchem Umfang? → siehe Anlage LMZ paedML
	3) Können die Log-Dateien / Konsolprotokolle nach bestimmten Kriterien ausgewertet werden? → siehe Anlage LMZ paedML Novell

[1] http://de.wikipedia.org/wiki/Authentifizierung

Merkmal	Beschreibung
4.Benutzerkontrolle → zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können	1) Verfahren zur Identifizierung und Authentifizierung (auch Fernwartung; Fernadministration) → siehe Anlage LMZ paedML Hinweis: Wie werden unberechtigter Benutzer abgewiesen?
	2) Werden unpersönliche Logins auch zu administrativen Zwecken verwendet? Hinweis: Derzeit werden von der paedML keine persönlichen administrativen Accounts unterstützt.
	3) Wie komplex ist das Passwort der Benutzer (speziell Adminpasswort) und in welchen Intervallen wird das Passwort geändert? → Hinweise LfD bzw. Materialen LfB-Server Das Passwort für administrative Account wird alle drei Monate geändert.
	4) Für wen wird die Nutzung der paedML wie zeitlich eingeschränkt? Hinweis: Die Nutzung der paedML unterliegt derzeit aufgrund der Nutzungsmöglichkeiten von Zuhause aus keiner zeitlichen Beschränkung.
	5) Wird der Arbeitsplatz (für Admin PC), an dem personenbezogene Daten verarbeitet werden durch eine automatische oder manuelle Dunkelschaltung des Bildschirms (Freischaltung nur über Passworteingabe) abgesichert? Hinweis: Im Rahmen des Unterrichts werden keine personenbezogenen Daten elektronisch erhoben bzw. verwaltet. Personenbezogene Daten werden im päd. Netz von Seminarlehrkräften nur an speziellen PCs erfasst, die in den Fach- bzw. Bereichsleiterzimmern stehen. Auf diesen Rechnern ist der Bildschirmschoner inkl. Passwortschutz aktiv (5 Minuten) aktiv. Des Weiteren kann der PC mit Hilfe der Tastenkombination [Strg] [Alt] [Einfg] gesperrt werden.
5.Zugriffskontrolle → zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.	1) Verfahren zur Identifizierung und Authentifizierung → siehe Anlage LMZ paedML
	2) Beschreibung der Autorisierung (differenzierte Berechtigungen: Rollen und Zugriffsrechte) bei der Nutzung der paedML → siehe Anlage LMZ paedML Hinweis: In dieser Anlage wird beschrieben, welche Benutzer / Benutzergruppe wie (lesend / schreibend / löschend) auf welche personenbezogene Daten welcher Betroffener zugreifen können. Der Lehrerzugriff nur auf bestimme Schülerhomeverzeichnisse kann derzeit in der paedML technisch nicht geregelt werden (siehe Punkt 10 organisatorische Regelung).
6.Übermittlungskontrolle → zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.	- Entfällt Hinweis: Erhält der Netzwerkberater von der Schulverwaltung eine Liste der neuen Schüler, um die Accounts in der paedML anlegen zu können, so ist diese keine Übermittlung im Sinne des LDSG.

Merkmal	**Beschreibung**
7.Eingabekontrolle → zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind.	1) Welche Person/Personen sind für die Kontrolle verantwortlich (paedML Benutzerverwaltung)? Hinweis: Dies ist i. d. R. der Netzwerberater an der Schule
	2) Welche Benutzer wurde wann von wem angelegt bzw. gelöscht? Hinweis: Der Netzwerberater legt die neuen Schüler zum Schuljahresbeginn an und löscht die Schüler die die Schule verlassen haben.
	3) Findet eine automatische Protokollierung der Eingaben in Log-Dateien statt? → siehe Anlage LMZ paedML
	4) Wie wird die inhaltliche Änderung von Dateien protokolliert? Beispiel: Ein Lehrer öffnet unterrichtsbezogen eine Textdatei in einem Schülerhomeverzeichnis und nimmt darin Änderungen vor. Da in den Metainformationen der Datei die Änderung automatisch vom Textverarbeitungsprogramm protokolliert wird, ist eine darüber hinausgehende Protokollierung nicht mehr notwendig.
8. Auftragskontrolle → zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	1) Existieren Verträge für folgende Formen der Auftragsdatenverarbeitung (siehe auch LDSG § 7 Abs 2)? ( ) Wartung/Fernwartung ( ) Administration/Fernadministration
	2) Die Verarbeitung personenbezogener Daten im Auftrag erfolgt nur entsprechend den Weisungen des Auftraggebers und wird durch folgende Maßnahmen gewährleistet: ( ) Schriftliche Weisungen ( ) Angebot und Auftragsbestätigung ( ) Der Auftraggeber erhält alle Datenausgaben zur Kontrolle.
	3) Wie wird bei Änderungen im Verfahrensablauf/Programmänderungen durch den Auftragnehmer verfahren?
	4) Welche Maßnahmen werden zur Sicherung der Fernwartung/Fernadministration angewendet? ( ) Ereignisauslösung vom Auftraggeber ( ) Rückrufautomatik ( ) Einmal-Passwort ( ) Protokollierung ( ) Virtual Private Network (VPN) ( ) Sonstige Maßnahmen:
	5) Wer kontrolliert in welcher Weise?

Merkmal	**Beschreibung**
9.Transportkontrolle → zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern die Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können, Hinweis: Bereich der Schule (Hoheitsgebiet) wird verlassen	1) Datenübertragung per WLAN - Wie erfolgt die Identifizierung und Authentifizierung der Benutzer? - Nach welchem Standard wird die Datenübertragung verschlüsselt? - Auf welche Daten kann der Benutzer zugreifen? Hinweis: Das päd. Netz und WLAN-Netz werden per VLAN Konfiguration auf den entsprechenden aktiven Komponenten logisch getrennt. Der Datenverkehr ist nach WPA2 verschlüsselt. Die Authentifizierung erfolgt verschlüsselt per LDAPS gegenüber der paedML Benutzerverwaltung.
	2) Zugriff von außen auf das Schulnetz - Wie erfolgt die Identifizierung und Authentifizierung der Benutzer? - Nach welchem Standard wird die Datenübertragung verschlüsselt? - Auf welche Daten kann der Benutzer zugreifen?
10.Verfügbarkeitskontrolle → zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind	1) Welches Verfahren zur Datensicherung wird eingesetzt (Datensicherungskonzept)? ( ) Notfallplan (Disaster and Recovery) ( ) Wöchentliches Backup von Home- /Tauschverzeichnissen auf eine separate USB-Festplatte ( ) Monatliches Backup des Servers (per Imageverfahren)
	2) Welche Maßnahmen gegen Spannungsprobleme wurden realisiert? ( ) Unterbrechungsfreie Stromversorgung USV) ( ) Überspannungsfilter
	3) Welche Brandschutzmaßnahmen wurden ergriffen? ( ) Brandmeldeanlage ( ) Handfeuerlöscher
	4) Welche weiteren Maßnahmen wurden umgesetzt (z. B. Virenschutz)? ( ) Virenschutz auf den Clients ( ) Virenschutz auf dem Server ( ) Virensoftware wird regelmäßig aktualisiert ( ) Virensoftware kann vom Benutzer nicht deaktiviert werden
11.Organisationskontrolle → die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird	1) Durch organisatorische Maßnahmen wird gewährleistet, dass den besonderen Anforderungen des Datenschutzes Rechnung getragen wird. ( ) Nutzungsordnung ( ) Aufgabenbeschreibung Netzwerkberater ( ) Dienstanweisung Folgende Regelung bzgl. des Zugriffs der Lehrer auf die Schülerhome-verzeichnisse wurde getroffen …. ( ) Schulung der Kollegen (z.B. Truecrypt)

Merkmal	Beschreibung
	( ) An der Schule / am Seminar gibt es eine Person, die die Aufgaben des behördlichen Datenschutzbeauftragten wahrnimmt. ( ) An der Schule / am Seminar gibt es einen behördlichen Datenschutzbeauftragten.